DataStar Web

Documents

Table of Contents

Differential cryptanalysis of DES-like cryptosystems.

Accession number & update
4070571, C9202-6130S-089; 920000.
Author(s)
Biham-E; Shamir-A.
Author affiliation
Dept of Appl Math & Comput Sci, Weizmann Inst of Sci, Rehovot, Israel.
Source
Journal-of-Cryptology (USA), vol.4, no.1, p.3-72, 1991.
CODEN
JOCREQ.
ISSN
ISSN: 0933-2790.
Publication year
1991.
Language
EN.
Publication type
J Journal Paper.
Treatment codes
P Practical; T Theoretical or Mathematical.
Abstract
The Data Encryption Standard (DES) is the best known and most widely used cryptosystem for civilian applications. It was developed at IBM and adopted by the National Bureau of Standards in the mid 1970s, and has successfully withstood all the attacks published so far in the open literature. The authors develop a new type of cryptanalytic attack which can break the reduced variant of DES with eight rounds in a few minutes on a personal computer and can break any reduced variant of DES (with up to 15 rounds) using less than 2/sup 56/ operations and chosen plaintexts. The new attack can be applied to a variety of DES-like substitution/permutation cryptosystems, and demonstrates the crucial role of the (unpublished) design rules. (20 refs).
Descriptors
cryptography; iterative-methods; standards.
Keywords
differential cryptanalysis; iterated cryptosystems; Data Encryption Standard; DES; cryptosystem; cryptanalytic attack; reduced variant.
Classification codes
C6130S (Data security).

S arch strategy

No.	Database	Search term	Info added since	Results
1	INZZ	invertible ADJ key ADJ schedule	unrestricted	0
2	INZZ	invertible AND key AND schedule	unrestricted	0
3	INZZ	invertible ADJ process	unrestricted	2
4	INZZ	invertible ADJ cryptanalysis ADJ process	unrestricted	0
5	INZZ	invertible AND process	unrestricted	124
6	INZZ	5 AND cryptogrpahy	unrestricted	0
7	INZZ	5 AND key ADJ schedule	unrestricted	0
8	INZZ	5 AND security	unrestricted	4
9	INZZ	koyama	unrestricted	139
10	INZZ	kkoyama	unrestricted	0
11	INZZ	koyamak	unrestricted	0
12	INZZ	9 AND terada	unrestricted	2
13	INZZ	different ADJ order ADJ s ADJ boxes	unrestricted	0
14	INZZ	biham AND shamier	unrestricted	0
15	INZZ	biham AND shamir	unrestricted	18
16	INZZ	15 AND (sbox$ OR s-box$)	unrestricted	0
17	INZZ	biham-$.AU. AND shamir-$.AU.	unrestricted	9

Saved: 18-Nov-2004, 15:04:49 CET